UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Cultivating and Assessing
Information Security Culture

by

Adéle da Veiga

Thesis

submitted in fulfilment of the requirements for the degree
Doctor of Philosophy

in the subject of
Information Technology

in the
Faculty of Engineering, Built Environment and Information Technology
at the
University of Pretoria

Supervisor
Prof. J.H.P. Eloff

September 2008

© University of Pretoria

Abstract

The manner in which employees perceive and interact (behave) with controls implemented to protect information assets is one of the main threats to the protection of such assets and the effective use of information security controls. Should the interaction not be conducive to the protection of the information assets, it could have a profound impact on the profit of an organisation, productive working hours could be lost, confidential information might be disclosed to unauthorised people and compliance with legal and regulatory regulations could be affected – all this, despite the fact that adequate technical and procedural controls might be in place.

Current research highlights the importance of a strong information security culture to address the threat that employee behaviour poses to the protection of information assets. Various research perspectives propose how an acceptable level of information security culture should be cultivated, and how to assess this culture to determine whether it is on an acceptable level. These approaches are however not adequate to cultivate information security culture, as all the relevant information security components and the influences on the information security culture have to be considered. This leads to the question as to whether the assessment instruments proposed to assess the information security culture are indeed adequate and valid.

The main contribution of this research relates to the development of an information security culture framework and process consisting of an assessment instrument to assess information security culture. In order to develop the information security culture framework, the researcher developed a Comprehensive Information Security Framework (CISF) that equips organisations with a holistic approach to the implementation of information security. The framework provides a single point of reference for the governance of information security.

The Information Security Culture Framework (ISCF) is developed using the CISF as foundation. The ISCF can be used by organisations to cultivate an

information security culture conducive to the protection of information assets. It considers all the components required for information security culture, namely information security, organisational culture and organisational behaviour. It integrates the aforementioned concepts and illustrates the influence between the components.

The ISCF further serves as a basis for designing an information security culture assessment instrument. This instrument is incorporated as part of an Information Security Culture Assessment process (ISCULA) defined by the researcher. ISCULA provides management with the steps to conduct an information security culture assessment, as well as the steps to validate the assessment instrument.

The application of ISCULA is tested in an empirical study conducted in an organisation. It illustrates how to validate an information security culture assessment instrument by ensuring that it is designed based on the ISCF and meets the statistical requirements for a valid and reliable assessment instrument. Both the ISCF and the ISCULA process can ultimately be deployed by organisations to minimise the threat that employee behaviour poses to the protection of information assets.

Summary

Title: Cultivating and assessing information security culture

Candidate: Adéle da Veiga

Supervisor: Prof. J.H.P. Eloff

Department: Department of Computer Science, Faculty of Engineering, Built Environment and Information Technology

Degree: Doctor of Philosophy in Information Technology

Keywords: Information security, information security culture, cultivate, assess, framework, organisational culture, organisational behaviour, questionnaire, process

I dedicate this thesis to my husband, Willem.

Acknowledgements

First of all, I give praise to the Lord who gave me the strength and ability to perform this research study.

Furthermore, I would also like to express my sincere thanks to the following persons for their respective contributions:

- My parents, Nico and Ellen, who provided me with support and motivation throughout my life and instilled qualities in me that enabled me to complete this study;

- My husband, Willem, daughter, Shadonise, and son, Tiago, for their support and understanding during the completion of this thesis;

- My promotor, Professor Jan Eloff, for his motivation, wisdom and excellent guidance, and especially for the manner in which he inspired the best in me;

- Rina Owen, who assisted with the statistical analysis of the survey results;

- Isabel Claassen, for the efficient manner in which she performed the language editing of the thesis;

- the Organisational Diagnostics personnel who assisted with the empirical study and reporting of the results; and

- all the organisations that participated in the research study and thus ensured the success thereof.

PART I

Chapter 1 Introduction

1.1 Introduction 1
1.2 Background to and motivation for the research 1
1.2.1 What is an information security culture? 2
1.2.2 Why is an information security culture necessary? 3
1.2.3 Cultivating an information security culture 4
1.2.4 Assessing an information security culture 6
1.3 Problem statement 9
1.3.1 Research questions 9
1.4 Research scope 10
1.5 Research methodology 12
1.6 Terminology used 14
1.6.1 Information Security 14
1.6.2 Organisational or employee behaviour 15
1.6.3 Organisational culture 16
1.6.4 Organisational assets 16
1.7 Layout of thesis 16

Chapter 2 Defining an Information Security Culture

2.1 Introduction 19
2.2 Definition of an information security culture 10
2.2.1 The Information Security Forum 10
2.2.2 Schlienger and Teufel 20
2.2.3 Martins and Eloff 21
2.2.4 Summary of the definitions of information security culture 22
2.3 Comparing the different information security culture definitions 23
2.4 Information security culture as defined for this research study 25
2.5 Conclusion 25

Chapter 3 Current Research Perspectives

3.1 Introduction 27
3.2 Current perspectives on information security culture research 27
3.2.1 The scope of current perspectives on information security

culture research 28
3.2.2 Current perspectives on information security culture research – contributions and limitations....................................32
3.2.3 Gaunt...39
3.2.3.1 Contributions and limitations of Gaunt's perspective ...40
3.2.4 Nosworthy...40
3.2.4.1 Contributions and limitations of Nosworthy's perspective 41
3.2.5 Information Security Forum 41
3.2.5.1 Contributions and limitations of the ISF's perspective 42
3.2.6 Martins and Eloff...42
3.2.6.1 Contributions and limitations of Martins and Eloff's perspective 43
3.2.7 Kuusisto, Helokunnas and Ilvonen..44
3.2.7.1 Contributions and limitations of Kuusisto, Helokunnas and Ilvonen's perspectives......................45
3.2.8 Zakaria and Gani 46
3.2.8.1 Contributions and limitations of Zakaria and Gani's perspective 47
3.2.9 Schlienger and Teufel...48
3.2.9.1 Contributions and limitations of Schlienger and Teufel's perspective..49
3.2.10 The Organisation for Economic Co-operation and Development (OECD)...49
3.2.10.1 Contribution and limitations of the OECD's perspective 50
3.2.11 Tessem and Skaraas..50
3.2.11.1 Contribution and limitations of Tessem and Skaraas's perspective...52
3.2.12 Dojkovski, Lichtenstein and Warren..52
3.2.12.1 Contributions and limitations of Dojkovski, Lichtenstein and Warren's perspectives 54
3.2.13 Thomson, Von Solms and Louw 55

3.2.13.1 Contributions and limitations of Thomson, Von Solms and Louw's perspective 56
3.2.14 Kraemer and Carayon 56
3.2.14.1 Contributions and limitations of Kraemer and Carayon's perspective 57
3.2.15 Ruighaver, Maynard and Chang 57
3.2.15.1 Contributions and limitations of Ruighaver, Maynard and Chang's perspective 57
3.2.16 Van Niekerk and Von Solms 58
3.2.16.1 Contributions and limitations of Van Niekerk and Von Solms's perspective 59
3.2.17 Summary 59
3.3 Conclusion 61

PART II

Chapter 4 A Framework for Information Security

4.1 Introduction 63
4.2 Information security approaches 63
4.2.1 Existing information security approaches 65
4.2.2 ISO/IEC 17799 and ISO/IEC FDIS 27001 67
4.2.3 PROTECT 69
4.2.4 Capability Maturity Model 70
4.2.5 Information Security Architecture (ISA) 71
4.2.6 Standard of Good Practice for Information Security (SOGP) 71
4.3 Investigation of information security approaches 72
4.3.1 Defining the information security components 74
4.3.2 Discussion of the investigation into information security approaches 81
4.4 Proposed Information Security Framework 82
4.5 Conclusion 86

Chapter 5 A Framework for Information Security Culture

5. 1. Introduction 87

5. 2. A framework for information security culture..87
5.2.1 Information security culture and organisational culture..............88
5.2.2 The interaction between information security, behaviour and culture 89
5.2.2.1 Level 1 - Influencing information security behaviour and cultivating an information security culture.............89
5.2.2.2 Level 2 - Influencing information security behaviour and cultivating an information security culture.............91
5.2.2.3 Level 3 – Information Security Culture Framework 94
5. 3. Applying the Information Security Culture Framework..........................98
5. 4. Benefits of the Information Security Culture Framework.....................101
5. 5. Conclusion 102

PART III

Chapter 6 A Process for Assessing Information Security Culture

6.1 Introduction..103
6.2 Assessing the information security culture in an organisation 103
6.2.1 Benefits of questionnaire and survey measures 104
6.3 Background on processes to assess information security culture 106
6.3.1 Schlienger and Teufel...106
6.3.2 Martins and Eloff..107
6.4 Proposed process to assess information security culture...................109
6.4.1 Step 1: Information security culture assessment planning and preparation..111
6.4.1.1 Step 1.1: Involve stakeholders.................................111
6.4.1.2 Step 1.2: Develop an information security culture assessment instrument 112
6.4.1.3 Step 1.3: ISCF validation 113
6.4.1.4 Step 1.4: Determine population and sample size......119
6.4.1.5 Step 1.5: Conduct a pilot study 120
6.4.1.6 Step 1.6: Select appropriate assessment technology120
6.4.2 Step 2: Information security culture assessment administration..121
6.4.2.1 Step 2.1: Communicate information security culture

assessment 121
6.4.2.2 Step 2.2: Send out information security culture assessment instrument 121
6.4.2.3 Step 2.3: Monitor responses 122
6.4.3 Step 3: Information security culture assessment data analysis 122
6.4.3.1 Step 3.1: Conduct a statistical analysis 122
6.4.3.2 Step 3.2: Construct validity....................................... 123
6.4.3.3 Step 3.3: Reliability.. 125
6.4.4 Step 4: Information security culture assessment report writing and feedback 126
6.4.4.1 Step 4.1: Compile an information security culture assessment feedback report 126
6.4.5 Step 5: Implement information security culture assessment action plans... 127
6.4.5.1 Step 5.1: Information security awareness programme 127
6.5 Conclusion.. 129

Chapter 7 An Empirical Study

7.1 Introduction.. 130
7.2 Background 130
7.3 Information on empirical study organisation 131
7.3.1 Background to organisation used for empirical study 131
7.4 Step 1: Information security culture assessment planning and organisation 132
7.4.1 Step 1.1: Involve stakeholders.. 132
7.4.2 Step 1.2: Develop an information security culture assessment instrument.. 132
7.4.3 Step 1.3: ISCF validation 133
7.4.4 Step 1.4: Determine population and sample size..................... 143
7.4.5 Step 1.5: Conduct a pilot survey 143
7.4.6 Step 1.6: Select appropriate assessment technology 145
7.5 Step 2: Information security culture assessment administration 145

7.5.1 Step 2.1: Communicate information security culture assessment 145
7.5.2 Step 2.2: Send out information security culture assessment instrument 147
7.5.3 Step 2.3: Monitor responses 147
7.6 Step 3: Information security culture assessment data analysis 148
7.6.1 Step 3.1: Conduct a statistical analysis 148
7.6.2 Step 3.2: Construct validity 150
7.6.3 Step 3.3: Reliability 151
7.7 Information security culture assessment report writing and feedback 152
7.7.1 Step 4.1: Compile an information security culture assessment feedback report 152
7.8 Empirical study evaluation 160
7.9 Conclusion 163

PART IV

Chapter 8 Conclusion

8.1 Introduction 165
8.2 Revisiting the problem statement 165
8.3 Main contribution 169
8.4 Limitations 171
8.4 Future research 172

Bibliography 175

Appendices 186
Appendix A – Information security culture assessment instrument
Appendix B – Initial Information security culture assessment instrument
Appendix C – Information security culture assessment report
Appendix D – Paper published in journal: Information security culture – validation of an assessment instrument
Appendix E – Paper published in journal : An information security governance framework

List of Figures

Figure 1.1 Layout of thesis..17
Figure 3.1 Research areas (layers)...29
Figure 3.2 Current research perspectives on information security culture 31
Figure 4.1 Comprehensive Information Security Framework (CISF).......................83
Figure 5.1 Level 1 – Influencing information security behaviour and cultivating an information security culture 90
Figure 5.2 Level 2 – Influencing information security behaviour and cultivating an information security culture 92
Figure 5.3 Level 3 – Information security Culture Framework (ISCF) 97
Figure 6.1 Process for assessing information security culture (Information Security Culture Assessment - ISCULA)..110
Figure 6.2 Information security culture change cycle 119
Figure 7.1 Information security culture assessment communication.......................146
Figure 7.2 Job levels...149
Figure 7.3 Length of service 149
Figure 7.4 Geographical areas..149
Figure 7.5 Statements about information security culture knowledge 153
Figure 7.6 Results for the information security culture dimensions 154

List of Tables

Table 2.1 A comparison of the key elements of an information security culture and the available definitions 24

Table 3.1 Research perspectives on an information security culture 34

Table 4.1 Components of an information security approach 73

Table 6.1 Content validity analysis of an existing questionnaire 115

Table 7.1 Information security culture questionnaire statements 137

Table 7.2 Information security culture survey – representative sample 147

Table 7.3 Results of the SEM analysis 151

Table 7.4 Results of the reliability analysis 151

Table 7.5 Recommendations for information security culture 157